history, i.e., metadata. A parenthetical category review of Example 5 shows: Records (objects) that have not been accessed (object content) within the last five years (environment content) are not allowed access by doctors (role).

[0089] Therefore, when:

[0090] Patient-Record: O

[0091] Roles: R={Doctor}

[0092] Operations: OP={view, append, copy}

[0093] Application Context:

[0094] Relationship: 5 years duration

[0095] lat: last access time;

[0096] System Context:

[0097] currentTime;

in a formal the role-Permission Assignment with Context Constraints may be written:

[0098] PA(Doctor, O, view) [[currentTime−lat(O)<=5-years]]

[0099] The above expression specifies that only when the expression within [[]] evaluates to true, can the user with the Doctor role view the object O.

Example 6

[0100] An anesthesiologist is allowed to view the genetic makeup records of a patient if and only if the elapsed time of an anesthetic application to the patient during surgery is three hours or greater.

[0101] For this constraint, even within the same session, the same role (Anesthesiologist) may have different access rights for the same object (the genetic makeup record) depending upon the request time (environmental content).

[0102] Patient-Record: O

[0103] Roles: R={Anesthesiologist}

[0104] Operations: OP={view, append, copy}

[0105] System Context:

[0106] anesthetic elapsed Time;

in a formal specification, the role-Permission Assignment with Context Constraints may be written:

[0107] PA(Anesthesiologist, O, view) [[3:00<=anesthetic elapsed Time]]

[0108] The above expression specifies that only when the expression within [[]] evaluates to true, can the user with the Anesthesiologist role view the object O.

[0109] While certain exemplary embodiments have been put forth to illustrate the present invention, these embodiments are not to be taken as limiting to the spirit or scope of the present invention which is defined by the appended claims.

We claim:

1. An RBAC method for a controlled computer system wherein permission constraints may be set on the access permissions of a role according to each and every type or combination of information including subject information, object information, and environment information before access to a requested object is granted.

2. The RBAC method according to claim 1 wherein the constraints are not limited to information contained within the controlled computer system.

3. The RBAC method according to claim 1 wherein a constraint can be written to dynamically alter access grant on a per request basis.

4. The RBAC method according to claim 1 wherein the information is based on extracted information.

5. The RBAC method according to claim 4 wherein the extracted information is internal to the controlled computer system and includes text extracted from the requested object.

6. The RBAC method according to claim 4 wherein the extracted information is external to the controlled computer system.

7. The RBAC method according to claim 4 wherein constraints are set based upon extracted subject content.

8. The RBAC method according to claim 4 wherein constraints are set based upon extracted environment content.

9. The RBAC method according to claim 1 wherein the information is an application context based upon subject content or object content or both.

10. The RBAC method according to claim 1 wherein the information is a system context based upon subject content or environment content or both.

11. The RBAC method according to claim 1 wherein constraints are evaluated on the role-permission assignment before every access grant without the reassignment of roles.

12. The RBAC method according to claim 1 wherein the constraints are specified using SQL.

13. The RBAC method according to claim 1 wherein the constraints are specified using Relational Algebra.

14. The RBAC method according to claim 1 wherein the constraints are specified using Prepositional Logic.

15. The RBAC method according to claim 1 wherein the constraints are specified using Relational Algebra.

16. The RBAC method according to claim 6 wherein the extracted information external to the controlled computer system is obtained via a search mechanism that uses crawlers.

17. The RBAC method according to claim 6 wherein the extracted information external to the controlled computer system is obtained via a search mechanism that uses a mediator.

18. The RBAC method according to claim 6 wherein the extracted information external to the controlled computer system is obtained via a search mechanism using text search engines.

19. The RBAC method according to claim 6 wherein the extracted information external to the controlled computer system is obtained via a search mechanism as used in database management systems.

20. The RBAC method according to claim 6 wherein the extracted information external to the controlled computer system is obtained via a search mechanism as used in reconciled structured repositories.

21. The RBAC method according to claim 6 wherein the extracted information external to the controlled computer system is obtained via a search mechanism as used in geospatial database searches.